What is claimed is:

1. A security system on a network, comprising:

intrusion detecting means for detecting an intrusion through an analysis of a packet, adding intrusion information associated with the intrusion into the packet, creating an active packet and transmitting the active packet to an address of an intruder which transmitted the packet; and

routing means for tracking the intrusion, for all routes through which the intruder passed, based on the active packet transmitted thereto from the intrusion detecting means, and filtering the packet associated with the intruder, thereby isolating the intruder,

wherein the routing means includes active nodes on a local networks of a user to be attacked and the intruder.

2. The system as recited in claim 1, wherein the intrusion detecting means includes

means for recognizing a local network from which the intrusion is originated, during the detection of the intrusion; and

means for notifying the intrusion of a filtering means in a local network to which the user to be attacked belongs and that in a local network to which the intruder belongs.

3. The system as recited in claim 2, wherein the intrusion detecting means includes:

collection means for collecting packets which pass therethrough;

analysis means for receiving the packet from the collecting means and determining whether the packet is one associated with intrusion or an active packet; and

processing means for processing the intrusion information or the active packet, which is received from the analysis means.

4. The system as recited in claim 3, wherein the processing means, if the data received from the analysis means is one associated with the intrusion information, creates an active packet associated with the intrusion information and transmits it to another local network, and if the data received from the analysis means is the active packet, analyzes whether the active packet is concerned with the intrusion information,

wherein if the intrusion is made via an authenticated server, the processing means creates a mobile agent, transmits the same to the server and retrieves information for the intruder.

5. The system as recited in claims 1, wherein the routing means includes:

filtering means for determining whether the packet is transmitted or not;

classifying means for determining whether the packet from

the filtering means is an active packet or an internet protocol (IP) packet, if the packet is the IP packet, forwarding the packet, and if the packet is the active packet, transmitting the packet to be executed at an active packet execution environment; and

means, if the packet classified by the classifying means is one associated with the intrusion information, for adding the packet information to be filtered to the filtering means and forwarding the packet through an IP forwarding engine.

6. A method for use in a security system, which comprising the steps of:

a) detecting an intrusion through an analysis of a packet, adding intrusion information associated with the intrusion into the packet, creating an active packet and transmitting the active packet to an address of an intruder which transmitted the packet; and

b) tracking the intrusion, for all routes through which the intruder passed, by sharing intrusion detection information detected at local network border routers each of which includes an active node, to thereby defense against the intrusion on a network to which the intruder belongs.

7. The method as recited in claim 6, wherein the step a) includes the steps of:

a1) determining whether there is a packet or not;

a2) determining, if there is the packet, whether the

packet is one associated with the intrusion information, and if so, creating an active packet associated with the intrusion information and transmitting it to another local network;

a3) analyzing, if the packet is the active packet, whether the active packet is concerned with the intrusion information; and

a4) determining whether the intrusion is made via an authenticated server, and if so, creating a mobile agent, transmitting the mobile agent to the server and retrieving information for the intruder.

8. The method as recited in claim 6, wherein the step b) includes the steps of:

b1) classifying, if the packet inputted to the local network border router is one to be transmitted by filtering, whether the packet is an active packet or an Internet protocol (IP) packet;

b2) if the packet is the IP packet, forwarding the packet; and

b3) if the packet is the active packet, determining, whether the packet is one associated with the intrusion information, and if so, storing the intrusion information and forwarding the packet.

9. A computer-readable recording medium storing instructions for executing a method for use in a security system including a processor, the method comprising the steps

of:

a) detecting an intrusion through an analysis of a packet, adding intrusion information associated with the intrusion into the packet, creating an active packet and transmitting the active packet to an address of an intruder which transmitted the packet; and

b) tracking the intrusion, for all routes through which the intruder passed, by sharing intrusion detection information detected at local network border routers each of which includes an active node, to thereby defense against the intrusion on a network to which the intruder belongs.